UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/419,240	10/15/1999	MAKOTO TATEBAYASHI	NAK1-BI69	9950

7590 09/02/2003

JOSEPH W PRICE
PRICE GESS & UBELL
2100 S E MAIN ST
STE 250
IRVINE, CA 92614

EXAMINER	
SONG, HOSUK	
ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 09/02/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/419,240	TATEBAYASHI ET AL.	
	Examiner	Art Unit	
	Hosuk Song	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 October 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3,7* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jovanovich et al.(US 5,703,950) in view of Matsumoto et al.(US 6,286,008).

Claim 1: Jovanovich disclose recording medium transmits an inherent key to the access apparatus in (fig.1 and col.4,lines 5-9). Note that Jovanovich disclose inherent key being information that is unique to the recording medium apparatus in (col.4,lines 6-7). Jovanovich disclose a transfer phase where after successful authentication, access apparatus encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus in (col.4,lines 46-55). Jovanovich disclose authenticating device specific key in (col.4,lines 35-36). However, Jovanovich does not specifically disclose mutually authenticating between two apparatus. Matsumoto's patent disclose mutual authentication method where two apparatus exchanges secret information in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only

intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Claim 2: Jovanovich disclose calculation mean where access apparatus includes a first authentication information generating means and judges whether recording medium apparatus is legitimate in the authentication phase in (fig.1,2). Jovanovich disclose generating authentication information and outputting the first authentication information to the recording medium in (col.4,lines 30-36). Jovanovich disclose calculating, generating and outputting first calculated authentication information to the access apparatus in (col.4,lines 30-59). Jovanovich discloses judging whether recording medium apparatus is legitimate from the first authentication information using the secretly transmitted inherently key in (col.4,lines 35-38).

Claims 3: Jovanovich does not disclose a calculating, generating and outputting second authentication information. Matsumoto's patent disclose calculating, generating and outputting second authentication information by way of mutual authentication in (fig.15). Note Matsumoto transmitting secret information such as device ID in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Claims 4,5,11,12: Jovanovich disclose prestoring the inherent key in (col.4,lines 20-23). Jovanovich does not disclose first decrypting mean where receiving the encrypted inherent key and generating a decrypted inherent key by applying a decryption algorithm. Official notice is taken that it is well known in the art to encrypt a key when transmitting over a network.

Encrypting scheme provides security since encrypted data transmission are much more difficult for an unauthorized party to intercept and access. Further, it is inherent that decryption algorithm must be deployed in order to decrypt data.

Claim 6: Jovanovich disclose a master key where first and second key is same in (col.4,lines 51-57).

Claims 7,8: neither Jovanovich nor Matsumoto disclose encrypting the inherent key according to the public key cryptosystem using the first key that is the public key. Official notice is taken that encrypting a key with public key system is well known in the art. One of ordinary skill in the art would be motivated to use public key cryptosystem because since it uses two keys rather than one key it is extremely secure and relatively simple to use. Further, public cryptography schemes relatively efficient digital signature mechanism. The key used to describe public verification function is typically much smaller than for the symmetric key counterpart.

Claims 9,10: Jovanovich discloses using a same key or master key in (col.4,lines 51-57). Jovanovich does not specifically disclose prestoring a second master key group that includes a plurality of master keys. It is inherent in system of Jovanovich to include second storage for storing plurality of master keys in other end in order to verify or authenticate its master key. Encrypting the inherent key is discussed in claim 4 rejection above.

Claims 13-15: Jovanovich discloses multiple device id storage in (fig.1) and requires multiple authentication scheme for each apparatus in order to verify and validates its devices.

Claim 16: Jovanovich does not disclose generating a random number as the first authentication information. Matsumoto patent disclose this features in (col.3,lines 30-44). It would have been obvious to person of ordinary skill in the art at the time invention was made to use random number as the authentication information taught in Matsumoto with authentication

method disclosed in Jovanovich because since random number is non-deterministic it provides security against repeated attacks or random attacks by the hackers. Further, even if random number is hijacked it is useless to the hackers because new number is generated and old number gets discarded.

Claims 17: Jovanovich disclose calculation mean where access apparatus includes a first authentication information generating means and judges whether recording medium apparatus is legitimate in the authentication phase in (fig.1,2). Jovanovich disclose generating authentication information and outputting the first authentication information to the recording medium in (col.4,lines 30-36). Jovanovich disclose calculating, generating and outputting first calculated authentication information to the access apparatus in (col.4,lines 30-59). Jovanovich discloses judging whether recording medium apparatus is legitimate from the first authentication information using the secretly transmitted inherently key in (col.4,lines 35-38).

Claim 18: Jovanovich does not disclose applying the second encryption algorithm to the second authentication information using the secretly transmitted inherent key. It is well known in the art to use more than one encryption algorithm to encrypt the data. One of ordinary skill in the art would be motivated to use more than encryption algorithm in order to deter data hacking by the intruders. Since each data varies, it is highly feasible to use different encryption scheme to protect its data. It is inherent that second decryption algorithm must be used for data decryption.

Claims 19,20: Jovanovich disclose prestoring the inherent key in (col.4,lines 20-23). Jovanovich does not disclose first decrypting mean where receiving the encrypted inherent key and generating a decrypted inherent key by applying a decryption algorithm. Official notice is taken that it is well known in the art to encrypt a key when transmitting over a network. Encrypting scheme provides security since encrypted data transmission are much more difficult

for an unauthorized party to intercept and access. Further, it is inherent that decryption algorithm must be deployed in order to decrypt data.

Claims 21,22: Jovanovich disclose recording medium transmits an inherent key to the access apparatus in (fig.1 and col.4,lines 5-9). Note that Jovanovich disclose inherent key being information that is unique to the recording medium apparatus in (col.4,lines 6-7). Jovanovich disclose a transfer phase where after successful authentication, access apparatus encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus in (col.4,lines 46-55). Jovanovich disclose authenticating device specific key in (col.4,lines 35-36). However, Jovanovich does not specifically disclose mutually authenticating between two apparatus. Matsumoto's patent disclose mutual authentication method where two apparatus exchanges secret information in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus. Reproducing the decrypted digital content is disclosed by Jovanovich in (col.4,lines 55-59).

Claims 23-31: Jovanovich does not specifically disclose dividing a digital content and generates an encrypted data block. Examiner asserts that generating a file key is well known in the art. File key allows user to recognize and locate how data is to be encrypted/decrypted from plurality of keys and files. Official notice is taken that block ciphering is well known in the art. Block cipher in which a key and algorithm are applied to a block of data for example 64

contiguous bits at once as group rather than to one bit at a time. In order for identical blocks of text do not get encrypted the same way in a message, it is common to apply the ciphertext from the previous encrypted block to the next block sequence. One of ordinary skill in the art would be motivated to use block ciphering in order to ensure that all subsequent blocks result in ciphertext that doesn't match that of the first encrypting which makes it difficult for hackers to defeat the system.

Claims 32: Jovanovich disclose recording medium transmits an inherent key to the access apparatus in (fig.1 and col.4,lines 5-9). Note that Jovanovich disclose inherent key being information that is unique to the recording medium apparatus in (col.4,lines 6-7). Jovanovich disclose a transfer phase where after successful authentication, access apparatus encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus in (col.4,lines 46-55). Jovanovich disclose authenticating device specific key in (col.4,lines 35-36). However, Jovanovich does not specifically disclose mutually authenticating between two apparatus. Matsumoto's patent disclose mutual authentication method where two apparatus exchanges secret information in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Claim 33: Jovanovich disclose calculation mean where access apparatus includes a first authentication information generating means and judges whether recording medium apparatus

is legitimate in the authentication phase in (fig.1,2). Jovanovich disclose generating authentication information and outputting the first authentication information to the recording medium in (col.4,lines 30-36). Jovanovich disclose calculating, generating and outputting first calculated authentication information to the access apparatus in (col.4,lines 30-59). Jovanovich discloses judging whether recording medium apparatus is legitimate from the first authentication information using the secretly transmitted inherently key in (col.4,lines 35-38).

Claim 34: Jovanovich does not disclose a calculating, generating and outputting second authentication information. Matsumoto's patent disclose calculating, generating and outputting second authentication information by way of mutual authentication in (fig.15). Note Matsumoto transmitting secret information such as device ID in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Claim 35: Jovanovich disclose recording medium transmits an inherent key to the access apparatus in (fig.1 and col.4,lines 5-9). Note that Jovanovich disclose inherent key being information that is unique to the recording medium apparatus in (col.4,lines 6-7). Jovanovich disclose a transfer phase where after successful authentication, access apparatus encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus in (col.4,lines 46-55). Jovanovich disclose authenticating device specific key in (col.4,lines 35-36). However, Jovanovich does not specifically disclose mutually authenticating between two apparatus. Matsumoto's patent

disclose mutual authentication method where two apparatus exchanges secret information in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Claim 36: Jovanovich disclose recording medium transmits an inherent key to the access apparatus in (fig.1 and col.4,lines 5-9). Note that Jovanovich disclose inherent key being information that is unique to the recording medium apparatus in (col.4,lines 6-7). Jovanovich disclose a transfer phase where after successful authentication, access apparatus encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus in (col.4,lines 46-55). Jovanovich disclose authenticating device specific key in (col.4,lines 35-36). However, Jovanovich does not specifically disclose mutually authenticating between two apparatus. Matsumoto's patent disclose mutual authentication method where two apparatus exchanges secret information in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Claim 37: Jovanovich does not disclose a calculating, generating and outputting second authentication information. Matsumoto's patent disclose calculating, generating and outputting second authentication information by way of mutual authentication in (fig.15). Note Matsumoto transmitting secret information such as device ID in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Claims 38-41: Jovanovich disclose recording medium transmits an inherent key to the access apparatus in (fig.1 and col.4,lines 5-9). Note that Jovanovich disclose inherent key being information that is unique to the recording medium apparatus in (col.4,lines 6-7). Jovanovich disclose a transfer phase where after successful authentication, access apparatus encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus in (col.4,lines 46-55). Jovanovich disclose authenticating device specific key in (col.4,lines 35-36). However, Jovanovich does not specifically disclose mutually authenticating between two apparatus. Matsumoto's patent disclose mutual authentication method where two apparatus exchanges secret information in (col.4,lines 1-19). It would have been obvious to person of ordinary skill in the art at the time invention was made to use mutual authentication method using a device ID disclosed in Matsumoto with device authentication method taught in Jovanovich because mutual authentication scheme ensures two parties that data is routed/forwarded to authorized destination only and further since it uses device specific ID to perform authentication, not only

intended recipient receives data but assures data is transmitted and received at only authorized specific apparatus.

Conclusion

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Davis (US 5,949,881) discloses activation method based on user authentication or device.

b. Kuroda et al.(US 6,421,779) discloses mutual authentication between two devices.

c. Schneier (Appled Cryptography) discloses mutual authentication and public key system

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Fri from 6:00 am- 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

HSS

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100